Ransomware has evolved into enterprise-grade malware that holds computers and data files hostage, locks down entire server systems swiftly, and brings productivity to a halt for days to months on end with large financial implications to the victim.

Cybercriminals are quick to exploit the global pandemic situation. There were over 304.7 million ransomware attacks in the first half year of 2021, already surpassing the full year total attacks of 2020. The U.S specifically suffered 227.3 million attempted attacks, which equates to 865 threats per minute in 2021. Recent reports suggest that 90% of financial institutions have been hit by ransomware. According to PayPal CEO Dan Schulman, financial services firms face a **billion** attempted attacks a year. The financial sector has been found to be amongst the hardest hit sectors, along with manufacturing, healthcare and professional services.

It's no secret why cyber criminals attack financial institutions with ransomware. The potential for a big payoff is hard to pass up. This entices Cyber criminals to target financial institutions because they hold the most sensitive detail on their customers and the implications of downtime mean victim organizations have historically paid the ransom. Financial institutions are also the backbone of our society and due to the interconnected nature of organizations today, the knock-on effects are significant globally.

Financial sector organisations such as banks and their service providers have always been at the forefront of enterprise cybersecurity. Their vital part in today's infrastructure and the massive amounts of consumer data has made them an appealing target for cybercriminals utilizing more and more advanced methods to circumvent existing prevention-based security. Financial institutions rely on their service providers to bring hassle-free technology, ensuring that banks and their critical data stay safe and available. Banks are a vital part of our society, and their service providers must do their utmost to be reliable, stable, but most importantly, bring forward the right technology.

With this being said, we've seen recent attacks on vendors such as Kaseya, Travelex, Pitney Bowes, Finastra, Cognizant, and Diebold Nixdort.

Cognizant and Finastra experienced ransomware attacks while planning for their workforce to work from home due to COVID-19. Finastra has over 8,500 customers and some of the world's largest banks as customers. Finastra was specifically targeted for it's customer base.

Travelex was so serious that it ultimately led to the company's bankruptcy and the loss of 1,300 jobs. The incident occurred when threat actors breached the network by exploiting unpatched vulnerabilities in VPN servers. Some customers were left stranded in foreign locations without local currency as a result of the disruptions – this level of disruption led to desperation to get their systems back and a $2.3m ransom was paid. As a result of the Travelex attack, a number of banks stopped customers ordering foreign currency, including HSBC, Lloyds, Barclays, Tesco Bank, Sainsbury's Bank, Virgin Money, First Direct and Royal Bank of Scotland.

The ransomware threat is paying its toll on banks specifically as it has evolved into enterprise-grade malware, locking down entire server systems swiftly. An example of this is BancoEstado, one of Chile's three biggest banks, who was forced to shut down all branches. It happened even though BancoEstado has experienced IT-teams and best-of-breed prevention-based solutions in place. They hoped to recover from the attack unnoticed, but the damage was pervasive as the cybercriminals locked up most servers and workstations. How did it all happen? An employee simply opened a malicious attachment that had ransomware in it.

The ransomware gang behind the Maze ransomware strain claims its reasons for attacking banks and tech vendors are virtuous: It's simply drawing attention to security lapses in the industry. Cognizant and Pitney Bowes were both victims of Maze, and the ransomware gang later said they performed a "routine check of previously accessed systems" and found that no changes had been made. "the security perimeter was a hole the size of the Channel tunnel," the press release said. "We decided not to block the work of the bank. It was at least incorrect during the world pandemic." However, the ransomware gang has multiple times since then showed they have no conscience. It's just a matter of time before they strike again.

On a daily basis, more advanced ransomware variants and threat groups are emerging, with the one goal in infiltrating organizations with their virus. Doing so provides them with access to proprietary data and infrastructure, meaning they then have the power to cause significant financial, operational and political damage. Once they bypass the typically rudimentary security applications, adversaries can inflict massive damage by charging high ransoms and bringing a halt to operations that are vital to the organization, but also to the global economy.

When BullWall's RansomCare (RC) is deployed, it detects the ransomwares illegitimate encryption immediately. No matter what time the attack takes place, an automated response is initiated, isolating the infected device and user and stopping the spread of illegitimate encryption to file shares, database and application servers. RC will automatically generate a report that provides you with full details of which files did manage to get encrypted so IT teams could restore from backup and fulfill potential obligations to data protection regulators very quickly. For any financial services institution, this means no concerns about downtime and minimal impact to operations. There would have been no financial losses relating to the attack as the ransom wouldn't have needed to be paid either.

RC acts as the Last Line of Defense to a variety of banks and financial institutions, our customers can be sure that productivity remains high, operations continue unhindered and the cost of downtime is minimized even if they're hit by a ransomware attack.